

Segurança de Redes

Varreduras
Analisadores de vulnerabilidades

Prof. Rodrigo Rocha
Prof.rodrigorocha@yahoo.com



Funcionamento de um ataque

- Levantamento de informações
  - footprint
  - fingerprint
  - varreduras
- Explorações
  - força bruta
  - exploits
  - sql injection, etc.
- Elevação de privilégios
- Instalação de backdoor e ferramentas
- Obtendo as informações privilegiadas

Verreduras

- Levantamento de informações sobre o sistema “alvo”;
- Podemos utilizar ferramentas automatizadas (muito “barulhenta”) ou manuais (menos “barulhentas”)
- Manual
  - telnet <porta> Ex: telnet 80
  - echo “teste” | nc www.alvo.com 80 | grep “<address>”

Varreduras - ferramentas

- NMAP
  - Sofisticado portscan (varredura de portas)
  - Escrito por Fyodor
  - Manual: http://nmap.org/man/pt-br/

root@charybdis.dubrawsky.org: /root

```
[root@charybdis /root]# nmap 10.16.17.236

Starting nmap V. 3.00 ( www.insecure.org/nmap/ )
Interesting ports on eomer.dubrawsky.org (10.16.17.236):
(The 1590 ports scanned but not shown below are in state: closed)
Port       State       Service
22/tcp     open        ssh
25/tcp     open        smtp
111/tcp    open        sunrpc
587/tcp    open        submission
665/tcp    open        unknown
898/tcp    open        unknown
4045/tcp   open        lockd
32776/tcp  open        sometimes-rpc15
32777/tcp  open        sometimes-rpc17
32778/tcp  open        sometimes-rpc19
32779/tcp  open        sometimes-rpc21

Nmap run completed -- 1 IP address (1 host up) scanned in 51 seconds
[root@charybdis /root]#
```



NMap – tipos de varreduras

- Sintaxe
  - nmap <parametros> host –p porta
  - Exemplo:
    - nmap 192.168.0.1
- Exemplos de uso
  - **Verificando o sistema operacional**
    - nmap 192.168.0.1 –O
  - **Não efetua ping (útil para firewall do windows)**
    - nmap 192.168.0.2 –P0
  - **Tentar obter a versão do serviço**
    - nmap 192.168.0.100 –sV
  - Varrer uma faixa de IP
    - nmap 10.0.0.1-100
  - Criar um log da varredua
    - nmap 10.0.0.1-254 –oN varretura.txt
  - Scaneando uma faixa de IP procurando uma determinada porta
    - nmap 10.0.0.1-250 –p 80



NMap – “Tentando” evitar Firewall/IDS

- **-T <Paranoid|Sneaky|Polite|Normal|Aggressive|Insane> (Estabelece um padrão de temporização)**
  - “Nmap oferece seis padrões de temporização. Você pode especificá-los com a opção -T e os números (0 - 5) ou os nomes. Os nomes de padrões são paranóico (paranoid, 0), furtivo (sneaky, 1), educado (polite, 2), normal (3), agressivo (agressive, 4) e insano (insane, 5). Os dois primeiros são para evitar um IDS. O modo educado (ou polido), diminui o ritmo de escaneamento para usar menos banda e recursos da máquina alvo. O modo normal é o padrão e, portanto, -T3 não faz nada. O modo agressivo acelera os scans assumindo que você está em uma rede razoavelmente rápida e confiável. Finalmente, o modo insano assume que você está em uma rede extraordinariamente rápida ou está disposto a sacrificar alguma precisão pela velocidade.”



NMap – “Tentando” evitar Firewall/IDS

- **-f (fragmenta os pacotes); --mtu (usando a MTU especificada)**
  - “A idéia é dividir o cabeçalho TCP em diversos pacotes para tornar mais difícil para os filtros de pacotes, os sistemas de detecção de intrusão, e outros aborrecimentos, detectar o que você está fazendo”
- **-D <chamariz1 [,chamariz2][,ME],...> (Disfarça um scan usando chamarizes)**
  - “Faz com que um scan com chamarizes seja executado, o que parece ao host remoto que, o(s) host(s) que você especificou como chamarizes também estejam escaneando a rede-alvo. Com isso, o IDS poderá reportar 5 a 10 scans de portas de endereços IP únicos, mas não saberá qual IP estava realmente escaneando e qual era um chamariz inocente. Embora isso possa ser desvendado através de rastreamento de caminho de roteador, descarte de respostas (response-dropping) e outros mecanismos ativos, normalmente é uma técnica eficaz para esconder o seu endereço IP.”

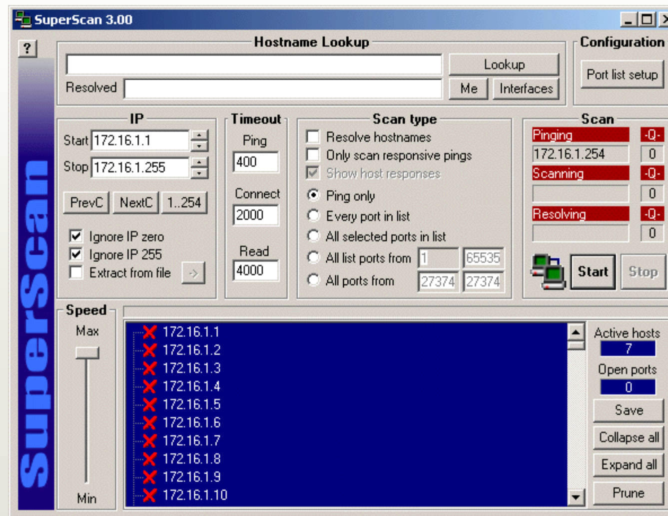


NMap – “Tentando” evitar Firewall/IDS

- **-S <Endereço_IP> (Disfarça o endereço de origem)**
  - “Em algumas circunstâncias, o Nmap pode não conseguir determinar o seu endereço de origem (o Nmap irá dizer se for esse o caso). Nesta situação, use o -S com o endereço IP da interface que você deseja utilizar para enviar os pacotes.
  - Outro uso possível para esta flag é para disfarçar o scan e fazer com que os alvos achem que alguma outra pessoa está escaneando-as. Imagine uma empresa que está constantemente sofrendo scan de portas de um concorrente! A opção -e normalmente seria requerida para este tipo de uso e -P0 seria recomendável.”
  - Fonte: Manual do NMAP

SuperScan (Windows)

- PortScanner



Banner grabber

- Retirar informações através do banner do aplicativo
  - telnet IP porta
  - Exemplo: telnet 192.168.0.100 21

```
[root@security ~]# telnet 192.168.0.1 21
Trying 192.168.0.1...
Connected to 192.168.0.1 (192.168.0.1).
Escape character is '^]'.
220 Microsoft FTP Service (Version 5.0).
```



HPING

- Enviar pacotes “montados” TCP
- hping alvo.com.br –p <porta>

- Opções
  - -F --fin set FIN flag
    -S –syn set SYN flag
    -R --rst set RST flag
    -P --push set PUSH flag
    -A --ack set ACK flag
    -U –urg set URG flag
    -X --xmas set X unused flag (0x40)
    -Y --ymas set Y unused flag (0x80)

  - -p <número porta>



Nessus

- Instalando
  - rpm –ivh Nessus-3.2.0-es5.i386.rpm
  - rpm –ivh Nessus-Client-3.2.0-es5.i386.rpm
- Criando o usuário
  - **/opt/nessus/sbin/nessus-add-first-user**
- **Carregando servidor nessus**
  - **/opt/nessus/sbin/nessusd -D &**
- **carregando Cliente**
  - **/opt/nessus/bin/NessusClient**



Paraos



John the Ripper

- Instalando
  - tar xzvf john-1.7.0.2.tar.gz
  - cd john-1.7.0.2/src
  - make clean linux-x86-any
  - cd ../run
- Utilizando
  - john arquivo_senhas
- Usando com dicionários
  - john arquivo_senhas --wordlist=./dicionario.txt



Senhas Windows

- bkhive-linux /mnt/hda1/WINDOWS/system32/config/system saved-syskey.txt
- samdump2-linux /mnt/hda1/WINDOWS/system32/config/sam saved-syskey.txt>password-hashes.txt
- john password-hashes.txt -w:eng.txt
- http://www.plain-text.info/search/



Bibliografia

- **Livro texto**
  - ANONIMO, .. **Segurança Máxima Totalmente Atualizado**. 3.ed. Rio de Janeiro: CAMPUS, 2005.
- **Complementar**
  - BURNETT, Steve; PAINE, Stephen. **Criptografia e Segurança**: o guia oficial RSA. 1.ed. São Paulo: Campus, 2002.
  - PETERSON, L.L. **Redes de Computadores**: uma abordagem de sistemas. 3.ed. Rio de Janeiro: Campus, 2004.
  - WADLOW, Thomas. **Segurança de Redes**: Projeto e Gerenciamento de Redes Segura. 1.ed. Rio de Janeiro: Campus, 2000.
  - SCHNEIER, Bruce. **Segurança.com: Segredos e Mentiras Sobre a Proteção na Vida Digital**. 1.ed. Rio de Janeiro: CAMPUS, 2001.